Zur Theorie der identischen Kongruenzen mit Idealmoduln.*)

Von László Zányi in Szeged.

Die von M. Bauer[1]) für ein Primzahlpotenzmodul aufgestellten Kongruenzen

$$\prod_r (x-r) \equiv (x^{p-1}-1)^{p^{\alpha-1}} \pmod{p^\alpha}$$

und

$$\prod_{i=1}^{m} (x-i) \equiv (x^p - x)^{\frac{m}{p}} \pmod{p^\alpha}$$

wo $m = p^\mu m'$, $(m', p) = 1$, und r das System aller verschiedenen, zu p^α teilerfremden Reste mod p^α durchläuft, hat H. S. Vandiver[2]) für einen zusammengesetzten Idealmodul verallgemeinert.

G. Rados[3]) hat statt der linearen Kongruenz eine binomische Kongruenz zugrunde gelegt und bewiesen, dass für jede ganze Zahl D und jede natürliche Zahl n die identische Kongruenz

$$(1^n - D)(2^n - D) \ldots ((p-1)^n - D) \equiv (D^{\frac{p-1}{\delta}} - 1)^\delta \pmod{p}$$

gilt, wo p eine beliebige Primzahl und $\delta = (n, p-1)$ ist.

*) Die vorliegende Arbeit ist eine abgekürzte, im wesentlichen unveränderte Wiedergabe meiner Inauguraldissertation aus dem Jahre 1929; sie ist in ungarischer Sprache unter dem Titel: *Az idealmodulusú algebrai kongruenciák elméletéhez*, Budapest, 1929 erschienen.

1) M. Bauer, A Fermat-féle kongruenciatétel elméletéhez, *Math. és Phys. Lapok*, **10** (1901), S. 145—152; M. Bauer, Sur les congruences identiques, *Nouvelles Annales de Mathematiques*, IV. Serie, **2** (1902), S. 256—264; M. Bauer, Az azonos kongruenciák elméletéhez, *Math. és Phys. Lapok*, **12** (1903), S. 159—160.

2) H. S. Vandiver, The generalized Lagrange indeterminate congruence for a composite ideal modulus, *Annals of Mathematics*, II. Series, **18** (1917), S. 115—119.

3) G. Rados, Sur une identité remarquable de la théorie des congruences binomes, *Rendiconti del Circolo Matematico di Palermo*, **46** (1922), S. 308—314

Ö. ORE[4]) hat diese Identität für eine ganze ganzzahlige rationale Funktion

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m$$

verallgemeinert, indem er bewies, dass

$$f(1^n) f(2^n) \ldots f((p-1)^n) \equiv Z(C_0, C_1, \ldots, C_{l-1})^\delta \pmod{p}$$

ist, wo

$$l = \frac{p-1}{\delta},$$

$$C_i = a_{m-i} + a_{m-i-l} + a_{m-i-2l} + \ldots$$

und

$$Z(C_0, C_1, \ldots, C_{l-1}) = \begin{vmatrix} C_0 & C_1 & \ldots & C_{l-1} \\ C_{l-1} & C_0 & \ldots & C_{l-2} \\ \vdots & \vdots & & \vdots \\ C_1 & C_2 & \ldots & C_0 \end{vmatrix}$$

eine zyklische Determinante ist.

Von M. BAUER[5]) rührt ein äusserst einfacher Beweis der RADOSschen Kongruenz, sowie eine Verallgemeinerung desselben her.

S. LUBELSKI[6]) bewies den Satz

$$\prod_{u=1}^{p^{m-1}} f(x-a+up) \equiv [f(x-a)]^{p^{m-1}} \pmod{p^m}$$

wo a eine beliebige ganze konstante Zahl und p eine beliebige ungerade Primzahl ist. Mit Hilfe dieses Satzes und der Anwendung des Resultantenbegriffes bewies er gewisse Verallgemeinerungen der BAUERschen (a. a. O. [1])), RADOSschen und ORESchen Sätze für einen ungeraden Primzahlpotenzmodul.

Der vorliegende Aufsatz enthält den Beweis einer identischen Kongruenz mit zusammengesetzten Idealmodul für Polynome, deren Koeffizienten Elemente eines Integritätsbereiches sind. Die VANDIVERsche, BAUERsche, RADOSsche und ORESche Sätze sind spezielle Fälle davon. Der LUBELSKIsche Satz ergibt sich durch eine einzige Division.

---

[4]) Ö. ORE, Note sur une identité dans la théorie des congruences supérieures, *Rendiconti del Circolo Matematico di Palermo*, **48** (1924), S. 37—40.

[5]) M. BAUER, Zur Theorie der identischen Kongruenzen (Aus Briefen an Herrn N. Tschebotarëw), *Bulletin de la Société Phys.-Math. de Kazan*, III. Serie, **3** (1928), S. 23—24.

[6]) S. LUBELSKI, Zur Theorie der höheren Kongruenzen, *Journal für die reine und angewandte Mathematik*, **162** (1930), S. 63—68.

1. Ist $\mathfrak{a}$ ein Ideal des algebraischen Zahlkörpers $\mathfrak{K}$ und

$$\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_k^{a_k},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ verschiedene Primideale dieses Körpers $\mathfrak{K}$ sind, so ist ein Repräsentantensystem der $\varphi(\mathfrak{a})$ zu $\mathfrak{a}$ teilerfremden Zahlklassen mod $\mathfrak{a}$ durch

$$\varkappa_{a_1}\varrho_1 + \varkappa_{a_2}\varrho_2 + \ldots + \varkappa_{a_k}\varrho_k \tag{1}$$

gegeben, wenn die $\varkappa_a$ von einander unabhängig die $\varphi(\mathfrak{p}^a)$ zu $\mathfrak{p}^a$ teilerfremden Zahlklassen mod $\mathfrak{p}^a$ durchlaufen und

$$\varrho_i \equiv 1 \pmod{\mathfrak{p}_i^{a_i}}, \quad \varrho_i \equiv 0 \left(\mod \frac{\mathfrak{a}}{\mathfrak{p}_i^{a_i}}\right)$$

ist. Desgleichen wird ein Repräsentantensystem für die $N(\mathfrak{a})$ Zahlklassen mod $\mathfrak{a}$ durch

$$\tau_{a_1}\varrho_1 + \tau_{a_2}\varrho_2 + \ldots + \tau_{a_k}\varrho_k \tag{2}$$

gegeben, wo die τ_a von einander unabhängig die $N(\mathfrak{p}^a)$ Zahlklassen mod $\mathfrak{p}^a$ durchlaufen.

Es sei $f(x)$ eine ganze rationale Funktion, deren Koeffizienten auch Unbestimmte oder ganze rationale Funktionen von Unbestimmten mit ganzen Koeffizienten aus $\mathfrak{K}$ sein können.

Untersuchen wir die Produkte $\prod_{\varkappa} f(\varkappa^n)$ und $\prod_{\tau} f(\tau^n)$, wo $\varkappa$ die zu $\mathfrak{a}$ teilerfremden und τ alle Zahlklassen mod $\mathfrak{a}$ durchläuft und n eine natürliche Zahl ist. Nach (1) und (2) wird

$$\prod_{\varkappa} f(\varkappa^n) \equiv \prod_{\varkappa_a} f(\varkappa_a^n)^{\frac{\varphi(\mathfrak{a})}{\varphi(\mathfrak{p}^a)}} \pmod{\mathfrak{p}^a}, \tag{3}$$

$$\prod_{\tau} f(\tau^n) \equiv \prod_{\tau_a} f(\tau_a^n)^{\frac{N(\mathfrak{a})}{N(\mathfrak{p}^a)}} \pmod{\mathfrak{p}^a}, \tag{4}$$

wo $\mathfrak{p}^a$ ein Primidealpotenzteiler des Ideals $\mathfrak{a}$ ist.

Ein Repräsentantensystem der zu $\mathfrak{p}^a$ teilerfremden Zahlklassen mod $\mathfrak{p}^a$ ist durch

$$\varkappa_1 + \pi\tau_1^{(1)} + \pi^2\tau_1^{(2)} + \ldots + \pi^{a-1}\tau_1^{(a-1)} \tag{5}$$

gegeben, wenn $\varkappa_1$ ein Repräsentantensystem der zu $\mathfrak{p}$ teilerfremden Zahlklassen mod $\mathfrak{p}$, die τ hingegen von einander unabhängig die $N(\mathfrak{p})$ Zahlklassen mod $\mathfrak{p}$ durchlaufen und π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbare und zu $\frac{\mathfrak{a}}{\mathfrak{p}^a}$ teilerfremde Zahl des Körpers

$\mathfrak{K}$ ist. Wir benützen die vollständige Induktion. Wir nehmen also an, dass

$$\prod_{x_{a-1}} f(x_{a-1}^n) \pmod{\mathfrak{p}^{a-1}}$$

schon bekannt ist, und beweisen, dass

$$\prod_{x_a} f(x_a^n) \equiv \prod_{x_{a-1}} f(x_{a-1}^n)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^a}$$

ist.

Nach (5) wird ein Repräsentantensystem der zu $\mathfrak{p}^a$ teilerfremden Zahlklassen durch

$$x_{a-1} + \pi^{a-1}\tau \qquad (a > 1)$$

gegeben, wenn x_{a-1} ein Repräsentantensystem der zu $\mathfrak{p}^{a-1}$ teilerfremden Zahlklassen mod $\mathfrak{p}^{a-1}$ und τ ein Repräsentantensystem der $N(\mathfrak{p})$ Zahlklassen mod $\mathfrak{p}$ durchlaufen. Demnach ist

$$(6) \qquad \prod_{x_a} f(x_a^n) \equiv \prod_{x_{a-1}} \prod_{\tau} f((x_{a-1} + \pi^{a-1}\tau)^n) \pmod{\mathfrak{p}^a}.$$

Nach dem binomischen Satze ist

$$f((x_{a-1} + \pi^{a-1}\tau)^n) \equiv f(x_{a-1}^n + n\pi^{a-1}x_{a-1}^{n-1}) \pmod{\mathfrak{p}^a},$$

wenn $a > 1$, und nach dem TAYLORschen Satze ist

$$f(x_{a-1}^n + n\pi^{a-1}x_{a-1}^{n-1}\tau) \equiv f(x_{a-1}^n) + n\pi^{a-1}x_{a-1}^{n-1}\tau f'(x_{a-1}^n) \pmod{\mathfrak{p}^a}.$$

Dies in (6) eingesetzt, erhalten wir

$$\prod_{x_a} f(x_a^n) \equiv \prod_{x_{a-1}} \prod_{\tau} [f(x_{a-1}^n) + n\pi^{a-1}x_{a-1}^{n-1}\tau f'(x_{a-1}^n)] \equiv$$

$$\equiv \prod_{\tau} \left[\prod_{x_{a-1}} f(x_{a-1}^n) + n\tau\pi^{a-1} \prod_{x_{a-1}} f(x_{a-1}^n) \cdot \sum_{x_{a-1}} \frac{f'(x_{a-1}^n)}{f(x_{a-1}^n)} x_{a-1}^{n-1} \right] \equiv$$

$$(7) \qquad \equiv \prod_{x_{a-1}} f(x_{a-1}^n)^{N(\mathfrak{p})} +$$

$$+ n\pi^{a-1} \prod_{x_{a-1}} f(x_{a-1}^n)^{N(\mathfrak{p})} \cdot \sum_{x_{a-1}} \frac{f'(x_{a-1}^n)}{f(x_{a-1}^n)} x_{a-1}^{n-1} \cdot \sum \tau \pmod{\mathfrak{p}^a}.$$

Weil das Repräsentantensystem der $N(\mathfrak{p}^a)$ Zahlklassen mod $\mathfrak{p}^a$ durch

$$\tau_{a-1} + \pi^{a-1}\tau$$

gegeben ist, so ist in ähnlicher Weise

$$(8) \qquad \prod_{\tau_a} f(\tau_a^n) \equiv \prod_{\tau_{a-1}} f(\tau_{a-1}^n)^{N(\mathfrak{p})} +$$

$$+ n\pi^{a-1} \prod_{\tau_{a-1}} f(\tau_{a-1}^n)^{N(\mathfrak{p})} \cdot \sum_{\tau_{a-1}} \frac{f'(\tau_{a-1}^n)}{f(\tau_{a-1}^n)} \tau_{a-1}^{n-1} \cdot \sum \tau \pmod{\mathfrak{p}^a}.$$

Die Elemente des Repräsentantensystems der $N(\mathfrak{p})$ Zahlklassen mit Ausnahme des Elementes 0 sind Wurzel der Kongruenz

$$x^{\varphi(\mathfrak{p})} \equiv 1 \pmod{\mathfrak{p}}.$$

Ist $\varphi(\mathfrak{p}) > 1$ resp. $N(\mathfrak{p}) > 2$, so folgt hieraus

$$\sum \tau \equiv 0 \pmod{\mathfrak{p}}.$$

Für $N(\mathfrak{p}) > 2$ und $a > 1$ wird also nach (7) und (8)

$$(9) \qquad \prod_{\varkappa_a} f(\varkappa_a^n) \equiv \prod_{\varkappa_{a-1}} f(\varkappa_{a-1}^n)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^a},$$

$$(10) \qquad \prod_{\tau_a} f(\tau_a^n) \equiv \prod_{\tau_{a-1}} f(\tau_{a-1}^n)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^a}.$$

Wir werden nun zeigen, dass für $a > 2$ diese Kongruenzen auch im Falle $N(\mathfrak{p}) = 2$ bestehen.

Im Falle $N(\mathfrak{p}) = 2$ besteht das Repräsentantensystem der zu $\mathfrak{p}$ teilerfremden Zahlklassen aus dem einzigen Elemente 1. Daher sind nach (5) die Elemente des Repräsentantensystems der zu $\mathfrak{p}^{a-1}$ teilerfremden Zahlklassen mod $\mathfrak{p}^{a-1}$ und deren n-te Potenzen $\equiv 1 \pmod{\mathfrak{p}}$. Also sind in (7) die Produkte

$$\frac{f'(\varkappa_{a-1}^n)}{f(\varkappa_{a-1}^n)} \varkappa_{a-1}^{n-1} \prod_{\varkappa_{a-1}} f(\varkappa_{a-1}^n)^{N(\mathfrak{p})}$$

alle derselben ganzen Grösse U kongruent (mod $\mathfrak{p}$). Weil $N(\mathfrak{p}) = 2 \equiv 0 \pmod{\mathfrak{p}}$, so folgt hieraus für $a > 2$

$$\prod_{\varkappa_{a-1}} f(\varkappa_{a-1}^n)^{N(\mathfrak{p})} \cdot \sum_{\varkappa_{a-1}} \frac{f'(\varkappa_{a-1}^n)}{f(\varkappa_{a-1}^n)} \varkappa_{a-1}^{n-1} \equiv \varphi(\mathfrak{p}^{a-1}) U \equiv 2^{a-2} U \equiv 0 \pmod{\mathfrak{p}}.$$

Demnach folgt aus (7) auch im Falle $N(\mathfrak{p}) = 2$ die Kongruenz (9), jedoch mit der Beschränkung $a > 2$.

Das Repräsentantensystem der $N(\mathfrak{p}) = 2$ Zahlklassen mod $\mathfrak{p}$ besteht aus den beiden Elementen 0, 1. Darum wird von den Repräsentanten der Zahlklassen mod $\mathfrak{p}^{a-1}$ und somit auch von ihren n-ten Potenzen die Hälfte $\equiv 0$ bezw. $\equiv 1 \pmod{\mathfrak{p}}$. Unter den Produkten

$$\frac{f'(\tau_{a-1}^n)}{f(\tau_{a-1}^n)} \tau_{a-1}^{n-1} \prod_{\tau_{a-1}} f(\tau_{a-1}^n)^{N(\mathfrak{p})}$$

sind also $\frac{1}{2} N(\mathfrak{p}^{a-1}) = 2^{a-2}$ derselben Grösse V und ebensoviele einer anderen Grösse W kongruent mod $\mathfrak{p}$. Dann ist aber für $a > 2$

$$\prod_{\tau_{a-1}} f(\tau_{a-1}^n)^{N(\mathfrak{p})} \cdot \sum_{\tau_{a-1}} \frac{f'(\tau_{a-1}^n)}{f(\tau_{a-1}^n)} \tau_{a-1}^{n-1} \equiv 2^{a-2}(V+W) \equiv 0 \pmod{\mathfrak{p}}.$$

Also folgt aus (8) auch im Falle $N(\mathfrak{p})=2$ die Kongruenz (10), jedoch mit der Beschränkung $a>2$.

Schreiben wir in (9) statt a den Exponenten $a-1$, so erhalten wir

$$\prod_{\varkappa_{a-1}} f(\varkappa_{a-1}^n) \equiv \prod_{\varkappa_{a-2}} f(\varkappa_{a-2}^n)^{N(\mathfrak{p})} \pmod{\mathfrak{p}^{a-1}}$$

oder

$$\prod_{\varkappa_{a-1}} f(\varkappa_{a-1}^n) \equiv \prod_{\varkappa_{a-2}} f(\varkappa_{a-2}^n)^{N(\mathfrak{p})} + \lambda \pmod{\mathfrak{p}^a},$$

wo λ eine durch $\mathfrak{p}^{a-1}$ teilbare ganze Zahl des Körpers $\mathfrak{K}$ ist. Folglich wird

$$\prod_{\varkappa_a} f(\varkappa_a^n) \equiv \left(\prod_{\varkappa_{a-2}} f(\varkappa_{a-2}^n)^{N(\mathfrak{p})} + \lambda\right)^{N(\mathfrak{p})} \equiv \prod_{\varkappa_{a-2}} f(\varkappa_{a-2}^n)^{N(\mathfrak{p}^2)} \pmod{\mathfrak{p}^a}.$$

Dieses Verfahren fortgesetzt erhalten wir:

$$(11) \qquad \prod_{\varkappa_a} f(\varkappa_a^n) \equiv \prod_{\varkappa_1} f(\varkappa_1^n)^{N(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}^a}, \quad \text{wenn } N(\mathfrak{p})>2;$$

$$(12) \qquad \prod_{\varkappa_a} f(\varkappa_a^n) \equiv \prod_{\varkappa_2} f(\varkappa_2^n)^{N(\mathfrak{p}^{a-2})} \pmod{\mathfrak{p}^a}, \quad \text{wenn } N(\mathfrak{p})=2.$$

In ähnlicher Weise wird

$$(13) \qquad \prod_{\tau_a} f(\tau_a^n) \equiv \prod_{\tau_1} f(\tau_1^n)^{N(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}^a}, \quad \text{wenn } N(\mathfrak{p})>2;$$

$$(14) \qquad \prod_{\tau_a} f(\tau_a^n) \equiv \prod_{\tau_2} f(\tau_2^n)^{N(\mathfrak{p}^{a-2})} \pmod{\mathfrak{p}^a}, \quad \text{wenn } N(\mathfrak{p})=2.$$

2. Es sei nun $a=1$, und untersuchen wir die Produkte $\prod_{\varkappa_1} f(\varkappa_1^n)$ und $\prod_{\tau_1} f(\tau_1^n)$ mod $\mathfrak{p}$, wo $\varkappa_1$ die zu $\mathfrak{p}$ teilerfremden und τ_1 alle Zahlklassen mod $\mathfrak{p}$ durchlaufen.

Wenn $(\varphi(\mathfrak{p}), n)=d$ ist, so folgt aus

$$\varkappa_{1i}^n \equiv \varkappa_{1k}^n \pmod{\mathfrak{p}}$$

die Kongruenz

$$\varkappa_{1i}^d \equiv \varkappa_{1k}^d \pmod{\mathfrak{p}}$$

und umgekehrt. Nun aber tritt bekanntlich in der Folge

$$\varkappa_{11}^d, \varkappa_{12}^d, \ldots, \varkappa_{1\varphi(\mathfrak{p})}^d$$

jeder d-te Potenzrest mod $\mathfrak{p}$ genau d-mal auf; also wird zufolge der soeben gemachten Bemerkung auch in der Folge

$$\varkappa_{11}^n, \varkappa_{12}^n, \ldots, \varkappa_{1\varphi(\mathfrak{p})}^n$$

jeder n-te Potenzrest mod $\mathfrak{p}$ genau d-mal auftreten. Wir bezeichnen die verschiedenen n-ten Potenzreste durch

$$\sigma_1,\ \sigma_2, \ldots, \sigma_l \quad \left(l = \frac{\varphi(\mathfrak{p})}{d}\right).$$

Ist

$$f(x) = \alpha_m x^m + \alpha_{m-1} x^{m-1} + \ldots + \alpha_0,$$

so ist zufolge der Kongruenz

$$\sigma_i^l \equiv 1 \pmod{\mathfrak{p}} \tag{15}$$

ersichtlich

$$f(\sigma_i) \equiv A_{l-1}\sigma_i^{l-1} + A_{l-2}\sigma_i^{l-2} + \ldots + A_1\sigma_i + A_0 \pmod{\mathfrak{p}},$$

wo

$$A_i = \alpha_i + \alpha_{i+l} + \alpha_{i+2l} + \ldots$$

und

$$\prod_{\varkappa_1} f(\varkappa_1^n) \equiv \prod_{i=1}^{l} f(\sigma_i)^d \pmod{\mathfrak{p}} \tag{16}$$

ist.

Bilden wir nun das Produkt der Determinanten

$$\Delta = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \sigma_1 & \sigma_2 & \ldots & \sigma_l \\ \sigma_1^2 & \sigma_2^2 & \ldots & \sigma_l^2 \\ \vdots & \vdots & & \vdots \\ \sigma_1^{l-1} & \sigma_2^{l-1} & \ldots & \sigma_l^{l-1} \end{vmatrix} \text{ und } Z(A_0, A_1, \ldots, A_{l-1}) = \begin{vmatrix} A_0 & A_1 \ldots A_{l-1} \\ A_{l-1} & A_0 \ldots A_{l-2} \\ \vdots & \vdots \quad \vdots \\ A_1 & A_2 \ldots A_0 \end{vmatrix},$$

so erhalten wir zufolge (15)

$$\Delta \cdot Z(A_0, A_1, \ldots, A_{l-1}) \equiv \Delta \cdot \prod_{i=1}^{l} f(\sigma_i) \pmod{\mathfrak{p}}.$$

Die VANDERMONDEsche Determinante Δ ist gleich dem Produkte der Differenzen $\sigma_i - \sigma_k$ $(i > k)$ und darum nicht teilbar durch $\mathfrak{p}$. Daher ist

$$\prod_{i=1}^{l} f(\sigma_i) \equiv Z(A_0, A_1, \ldots, A_{l-1}) \pmod{\mathfrak{p}}.$$

Nach (16) wird also

$$\prod_{\varkappa_1} f(\varkappa_1^n) \equiv Z(A_0, A_1, \ldots, A_{l-1})^d \pmod{\mathfrak{p}}. \tag{17}$$

Da das Repräsentantensystem der $N(\mathfrak{p})$ Zahlklassen mod $\mathfrak{p}$ vom

Repräsentantensystem der zu $\mathfrak{p}$ teilerfremden Zahlklassen sich durch das einzige Element 0 unterscheidet, so wird

$$(18)\qquad \prod_{\tau_1} f(\tau_1^n) \equiv f(0) \cdot Z(A_0, A_1, \ldots, A_{l-1})^d \pmod{\mathfrak{p}}.$$

Zufolge (17) resp. (18) können (11) und (13) auch so geschrieben werden:

$$(19)\qquad \prod_{\varkappa_a} f(\varkappa_a^n) \equiv Z(A_0, A_1, \ldots, A_{l-1})^{dN(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}},$$

$$(20)\qquad \prod_{\tau_a} f(\tau_a^n) \equiv f(0)^{N(\mathfrak{p}^{a-1})} Z(A_0, A_1, \ldots, A_{l-1})^{dN(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}},$$

wenn $N(\mathfrak{p}) > 2$ ist. Wird (19) in (3) und (20) in (4) eingesetzt, so ergibt sich wird

$$(21)\qquad \prod_{\varkappa} f(\varkappa^n) \equiv Z(A_0, A_1, \ldots, A_{l-1})^{d\frac{\varphi(\mathfrak{a})}{\varphi(\mathfrak{p})}} \pmod{\mathfrak{p}^a},$$

$$(22)\qquad \prod_{\tau} f(\tau^n) \equiv f(0)^{\frac{N(\mathfrak{a})}{N(\mathfrak{p})}} Z(A_0, A_1, \ldots, A_{l-1})^{d\frac{N(\mathfrak{a})}{N(\mathfrak{p})}} \pmod{\mathfrak{p}^a}.$$

In Anbetracht der Formeln (1), (2) für das Repräsentantensystem der zu $\mathfrak{a}$ teilerfremden resp. aller Zahlklassen mod $\mathfrak{a}$ wird

$$(23)\qquad \prod_{\varkappa} f(\varkappa^n) \equiv \sum_{i=1}^{k} \varrho_i Z(A_0, A_1, \ldots, A_{l_i-1})^{d_i\frac{\varphi(\mathfrak{a})}{\varphi(\mathfrak{p}_i)}} \pmod{\mathfrak{a}}$$

und

$$(24)\qquad \prod_{\tau} f(\tau^n) \equiv \sum_{i=1}^{k} \varrho_i f(0)^{\frac{N(\mathfrak{a})}{N(\mathfrak{p}_i)}} Z(A_0, A_1, \ldots, A_{l_i-1})^{d_i\frac{N(\mathfrak{a})}{N(\mathfrak{p}_i)}} \pmod{\mathfrak{a}}$$

wenn $N(\mathfrak{p}_i) > 2$ und $d_i = (\varphi(\mathfrak{p}_i), n)$, $l_i = \dfrac{\varphi(\mathfrak{p}_i)}{n}$ ist.

3. Untersuchen wir jetzt den Fall $N(\mathfrak{p}) = 2$. Es ist

$$(25)\qquad \prod_{\varkappa_1} f(\varkappa_1^n) \equiv f(1) \equiv \alpha_0 + \alpha_1 + \ldots + \alpha_m \pmod{\mathfrak{p}},$$

$$(26)\qquad \prod_{\tau_1} f(\tau_1^n) \equiv f(0) f(1) \equiv \alpha_0(\alpha_0 + \alpha_1 + \ldots + \alpha_m) \pmod{\mathfrak{p}}.$$

Das Repräsentantensystem der $\varphi(\mathfrak{p}^2) = 2$ gegen $\mathfrak{p}^2$ teilerfremden Zahlklassen mod $\mathfrak{p}^2$ wird durch

$$1, \quad 1 + \pi$$

gegeben. Diese befriedigen die Kongruenz

$$x^2 \equiv 1 \pmod{\mathfrak{p}^2};$$

daher ist

$$f(\varkappa_2) \equiv A_1 \varkappa_2 + A_0 \pmod{\mathfrak{p}^2},$$

wo

$$A_1 = \alpha_1 + \alpha_3 + \alpha_5 + \ldots, \quad A_0 = \alpha_0 + \alpha_2 + \alpha_4 + \ldots .$$

Es ist

$$(1+\pi)^n \equiv 1 + \pi n \pmod{\mathfrak{p}^2},$$

und darum

$$\prod_{\varkappa_2} f(\varkappa_2^n) \equiv f(1) f(1+\pi n) \equiv f(1)(f(1) + \pi n f'(1)) \pmod{\mathfrak{p}^2}.$$

Für ein gerades n wird πn durch $\mathfrak{p}^2$ teilbar und

$$\prod_{\varkappa_2} f(\varkappa_2^n) \equiv f(1)^2 \pmod{\mathfrak{p}^2};$$

also nach (12)

$$\prod_{\varkappa_a} f(\varkappa_a^n) \equiv f(1)^{2^{a-1}} \pmod{\mathfrak{p}^a}. \tag{27}$$

Ist aber n ungerade, also gleich $2n'+1$, so ist $\pi n \equiv \pi \pmod{\mathfrak{p}^2}$ und

$$\prod_{\varkappa_2} f(\varkappa_2^n) \equiv f(1)(f(1) + \pi f'(1)) \pmod{\mathfrak{p}^2}, \tag{28}$$

also nach (9)

$$\prod_{\varkappa_3} f(\varkappa_3^n) \equiv f(1)^2 (f(1) + \pi f'(1))^2 \pmod{\mathfrak{p}^3}, \tag{29}$$

$$\prod_{\varkappa_4} f(\varkappa_4^n) \equiv f(1)^4 (f(1) + \pi f'(1))^4 \equiv f(1)^{2^3} \pmod{\mathfrak{p}^4},$$

und allgemein

$$\prod_{\varkappa_a} f(\varkappa_a^n) \equiv f(1)^{2^{a-1}} \pmod{\mathfrak{p}^a} \quad \text{für } a > 3. \tag{30}$$

Ist n ungerade und 2 durch $\mathfrak{p}^2$ nicht teilbar, so können wir $\pi = 2$ nehmen; es wird dann

$$\prod_{\varkappa_2} f(\varkappa_2^n) \equiv f(1) f(3) \equiv f(1) f(-1) \equiv A_0^2 - A_1^2 \pmod{\mathfrak{p}^2}$$

und nach (12)

$$\prod_{\varkappa_a} f(\varkappa_a^n) \equiv (A_0^2 - A_1^2)^{2^{a-2}} \pmod{\mathfrak{p}^a} \quad \text{für } a > 1. \tag{31}$$

Das Repräsentantensystem der $N(\mathfrak{p}^2) = 4$ Zahlklassen mod $\mathfrak{p}^2$ wird durch

$$0,\ \pi,\ 1,\ 1+\pi$$

gegeben und daher

$$\prod_{\tau_2} f(\tau_2^n) \equiv f(0) f(\pi^n) \prod_{\varkappa_2} f(\varkappa_2^n) \qquad (\mathrm{mod}\ \mathfrak{p}^2).$$

Da

$$f(\pi^n) = \alpha_m \pi^{mn} + \alpha_{m-1} \pi^{(m-1)n} + \ldots + \alpha_2 \pi^{2n} + \alpha_1 \pi^n + \alpha_0$$

ist, so wird

$$f(\pi^n) \equiv \begin{cases} \alpha_0 & (\mathrm{mod}\ \mathfrak{p}^2) \quad \text{für } n > 1. \\ \alpha_0 + \pi\alpha_1 & (\mathrm{mod}\ \mathfrak{p}^2) \quad \text{für } n = 1. \end{cases}$$

Für ein gerades n wird daher

$$\prod_{\tau_2} f(\tau_2^n) \equiv \alpha_0^2 f(1)^2 \qquad (\mathrm{mod}\ \mathfrak{p}^2)$$

und nach (14) allgemein

$$(32) \qquad \prod_{\tau_a} f(\tau_a^n) \equiv (\alpha_0 f(1))^{2^{a-1}} \qquad (\mathrm{mod}\ \mathfrak{p}^a) \quad \text{für } a > 1.$$

Ist n ungerade und > 1, dann wird

$$(33) \qquad \prod_{\tau_2} f(\tau_2^n) \equiv \alpha_0^2 f(1)\,(f(1) + \pi f'(1)) \qquad (\mathrm{mod}\ \mathfrak{p}^2),$$

also nach (10)

$$(34) \qquad \prod_{\tau_3} f(\tau_3^n) \equiv \alpha_0^4 f(1)^2\,(f(1) + \pi f'(1))^2 \qquad (\mathrm{mod}\ \mathfrak{p}^3),$$

$$\prod_{\tau_4} f(\tau_4^n) \equiv \alpha_0^8 f(1)^4\,(f(1) + \pi f'(1))^4 \equiv \alpha_0^{2^3} f(1)^{2^3} \quad (\mathrm{mod}\ \mathfrak{p}^4),$$

und allgemein

$$(35) \qquad \prod_{\tau_a} f(\tau_a^n) \equiv (\alpha_0 f(1))^{2^{a-1}} \qquad (\mathrm{mod}\ \mathfrak{p}^a) \quad \text{für } a > 3.$$

Für $n = 1$ ist aber

$$(36) \qquad \prod_{\tau_2} f(\tau_2) \equiv \alpha_0 (\alpha_0 + \pi\alpha_1) f(1)\,(f(1) + \pi f'(1)) \qquad (\mathrm{mod}\ \mathfrak{p}^2),$$

also nach (10)

$$(37) \qquad \prod_{\tau_3} f(\tau_3) \equiv \alpha_0^2 (\alpha_0 + \pi\alpha_1)^2 f(1)^2\,(f(1) + \pi f'(1))^2 \qquad (\mathrm{mod}\ \mathfrak{p}^3),$$

$$\prod_{\tau_4} f(\tau_4) \equiv \alpha_0^4 (\alpha_0 + \pi\alpha_1)^4 f(1)^4\,(f(1) + \pi f'(1))^4 \equiv \alpha_0^{2^3} f(1)^{2^3} \quad (\mathrm{mod}\ \mathfrak{p}^4),$$

und allgemein

$$(38) \qquad \prod_{\tau_a} f(\tau_a) \equiv (\alpha_0 f(1))^{2^{a-1}} \qquad (\mathrm{mod}\ \mathfrak{p}^a) \quad \text{für } a > 3.$$

Ist n ungerade und 2 durch $\mathfrak{p}^2$ nicht teilbar, so können wir $\pi = 2$

nehmen und erhalten

$$\prod_{\tau_2} f(\tau_2^n) \equiv \alpha_0^2 (A_0^2 - A_1^2) \pmod{\mathfrak{p}^2} \quad \text{für } n > 1$$

und nach (14) allgemein

$$\prod_{\tau_a} f(\tau_a^n) \equiv [\alpha_0 (A_0^2 - A_1^2)]^{2^{a-2}} \pmod{\mathfrak{p}^a} \quad \text{für } a > 1,\ n > 1, \tag{39}$$

ferner

$$\prod_{\tau_2} f(\tau_2) \equiv \alpha_0 (\alpha_0 + 2\alpha_1)(A_0^2 - A_1^2) \pmod{\mathfrak{p}^2} \quad \text{für } n = 1$$

und nach (14) allgemein

$$\prod_{\tau_a} f(\tau_a) \equiv [\alpha_0 (\alpha_0 + 2\alpha_1)(A_0^2 - A_1^2)]^{2^{a-2}} \pmod{\mathfrak{p}^a} \quad \text{für } a > 1,\ n = 1. \tag{40}$$

Wenn wir (25), (27), (30) in (3) und (26), (32), (35), (38) in (4) einsetzen, so erhalten wir

$$\left.\begin{aligned} \prod_{\varkappa} f(\varkappa^n) &\equiv f(1)^{\varphi(\mathfrak{a})} \pmod{\mathfrak{p}^a} \\ \prod_{\tau} f(\tau^n) &\equiv (\alpha_0 f(1))^{\frac{N(\mathfrak{a})}{2}} \pmod{\mathfrak{p}^a} \end{aligned}\right\} \begin{array}{l} \text{für } n \equiv 0 \pmod 2,\ \mathfrak{p}^2 \mid 2,\ \mathfrak{p}^2 \nmid 2,\ a \geqq 1 \\ \text{und für } n \equiv 1 \pmod 2, \begin{cases} \mathfrak{p}^2 \mid 2,\ a = 1,\ a > 3, \\ \mathfrak{p}^2 \nmid 2,\ a = 1. \end{cases} \end{array}$$

Wird (31) in (3) und (39), 40 in (4) eingesetzt, so ergibt sich

$$\left.\begin{aligned} \prod_{\varkappa} f(\varkappa^n) &\equiv (A_0^2 - A_1^2)^{\varphi\frac{(\mathfrak{a})}{2}} \pmod{\mathfrak{p}^a} \\ \prod_{\tau} f(\tau^n) &\equiv [\alpha_0 (\alpha_0 + e\alpha_1)(A_0^2 - A_1^2)]^{\frac{N(\mathfrak{a})}{4}} \pmod{\mathfrak{p}^a} \end{aligned}\right\} \begin{array}{l} \text{für } n \equiv 1 \pmod 2, \\ \mathfrak{p}^2 \nmid 2,\ a > 1 \end{array}$$

wo

$$e = \begin{cases} 0 & \text{für } n > 1, \\ 2 & \text{für } n = 1. \end{cases}$$

Im Falle $n \equiv 1 \pmod 2$, $\mathfrak{p}^2 \mid 2$ hängt für $a = 2, 3$ das Produkt gemäss (28), (29), (33), (34), (36), (37) von der Wahl von π ab.

Jetzt können wir (23) und (24) für alle Fälle ergänzen und wir erhalten den folgenden

Satz. *Ist* $\mathfrak{a}$ *ein Ideal des algebraischen Zahlkörpers* $\mathfrak{K}$ *und*

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \ldots \mathfrak{p}_k^{a_k},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ *verschiedene Primideale dieses Körpers* $\mathfrak{K}$ *bedeuten, dann wird*

$$\prod_{\varkappa} f(\varkappa^n) \equiv \sum_{i=1}^{k} \varrho_i S_i \pmod{\mathfrak{a}},$$

$$\prod_{\tau} f(\tau^n) \equiv \sum_{i=1}^{k} \varrho_i T_i \pmod{\mathfrak{a}}.$$

Hier durchläuft $\varkappa$ *das Repräsentantensystem der zu* $\mathfrak{a}$ *teilerfremden Zahlklassen und* τ *das Repräsentantensystem aller Zahlklassen* mod $\mathfrak{a}$, *ferner ist*

$$f(x) = \alpha_m x^m + \alpha_{m-1} x^{m-1} + \ldots + \alpha_1 x + \alpha_0,$$

$$\varrho_i \equiv 1 \pmod{\mathfrak{p}_i^{\alpha_i}} \qquad \varrho_i \equiv 0 \left(\mathrm{mod}\ \frac{\mathfrak{a}}{\mathfrak{p}_i^{\alpha_i}}\right),$$

schliesslich haben S_i *und* T_i *die folgende Bedeutung. Wenn* $N(\mathfrak{p}_i) > 2$, *so ist für alle positive rationale ganze* n *und* a_i

$$S_i = Z(A_0, A_1, \ldots, A_{l_i-1})^{d_i \frac{\varphi(\mathfrak{a})}{\varphi(\mathfrak{p}_i)}}$$

$$T_i = [f(0) \,.\, Z(A_0, A_1, \ldots, A_{l_i-1})^{d_i}]^{\frac{N(\mathfrak{a})}{N(\mathfrak{p}_i)}}$$

wo $d_i = (\varphi(\mathfrak{p}_i), n)$, $l_i = \dfrac{\varphi(\mathfrak{p}_i)}{n}$, *ferner*

$$A_j = \alpha_j + \alpha_{j+l_i} + \alpha_{j+2l_i} + \ldots$$
$$(j = 0, 1, 2, \ldots, l_i - 1)$$

und

$$Z(A_0, A_1, \ldots, A_{l_i-1}) = \begin{vmatrix} A_0 & A_1 & \ldots & A_{l_i-1} \\ A_{l_i-1} & A_0 & \ldots & A_{l_i-1} \\ \vdots & \vdots & & \vdots \\ A_1 & A_2 & \ldots & A_0 \end{vmatrix}.$$

Wenn $N(\mathfrak{p}_i) = 2$, *so ist*

$$\left.\begin{aligned} S_i &= (\alpha_0 + \alpha_1 + \ldots + \alpha_m)^{\varphi(\mathfrak{a})} \\ T_i &= [\alpha_0(\alpha_0 + \alpha_1 + \ldots + \alpha_m)]^{\frac{N(\mathfrak{a})}{2}} \end{aligned}\right\} \begin{array}{l} \text{für } n \equiv 0 \pmod 2,\ \mathfrak{p}^2 \mid 2,\ \mathfrak{p}^2 \nmid 2,\ a_i \geqq 1 \\ \text{und für } n \equiv 1 \pmod 2,\ \begin{cases} \mathfrak{p}^2 \mid 2,\ a_i = 1,\ a_i > 3, \\ \mathfrak{p}^2 \nmid 2,\ a_i = 1\,; \end{cases} \end{array}$$

$$\left.\begin{aligned} S_i &= (A_0^2 - A_1^2)^{\frac{\varphi(\mathfrak{a})}{2}} \\ T_i &= [\alpha_0(\alpha_0 + e\alpha_1)(A_0^2 - A_1^2)]^{\frac{N(\mathfrak{a})}{4}} \end{aligned}\right\} \text{für } n \equiv 1 \pmod 2,\ \mathfrak{p}^2 \nmid 2,\ a_i > 1,$$

wo

$$e = \begin{cases} 0 & \text{für } n > 1, \\ 2 & \text{für } n = 1 \end{cases}$$

und

$$A_1 = \alpha_1 + \alpha_3 + \alpha_5 + \ldots, \qquad A_0 = \alpha_0 + \alpha_2 + \alpha_4 + \ldots.$$

Im Falle $N(\mathfrak{p}_i) = 2$, $n \equiv 1 \pmod 2$, $\mathfrak{p}^2 \mid 2$ *hängt für* $a_i = 2, 3$ *das Produkt von der Wahl des Repräsentanentsystems, welches* $\varkappa$ *bezw.* τ *durchlauft, ab.*

4. Anwendungen. 1. Der bewiesene Satz ist die Verallgemeinerung des ORESchen Satzes für zusammengesetzte Idealmoduln.

2. Es sei

$$f(x) = x - x$$

also

$$a_0 = A_0 = x, \quad a_1 = A_1 = -1, \quad a_2 = A_2 = 0, \ldots$$

und

$$Z(A_0, A_1, \ldots, A_{l_i-1}) = (-1)^{\frac{\varphi(\mathfrak{p}_i)}{d_i}} (x^{\frac{\varphi(\mathfrak{p}_i)}{d_i}} - 1).$$

Dann ist nach dem bewiesenen Satze

$$\prod_x (x - x^n) \equiv \sum_{i=1}^{k} \varrho_i S_i \pmod{\mathfrak{a}},$$

$$\prod_x (x - x^n) \equiv \sum_{i=1}^{k} \varrho_i T_i \pmod{\mathfrak{a}},$$

wo im Falle $N(\mathfrak{p}_i) > 2$ für $n \geqq 1$, $a_i \geqq 1$

$$S_i = (x^{\frac{\varphi(\mathfrak{p}_i)}{d_i}} - 1)^{d_i \frac{\varphi(\mathfrak{a})}{\varphi(\mathfrak{p}_i)}},$$

$$T_i = (x(x^{\frac{\varphi(\mathfrak{p}_i)}{d_i}} - 1)^{d_i})^{\frac{N(\mathfrak{a})}{N(\mathfrak{p}_i)}},$$

im Falle $N(\mathfrak{p}_i) = 2$ aber

$$\left.\begin{aligned} S_i &= (x-1)^{\varphi(\mathfrak{a})} \\ T_i &= (x^2 - x)^{\frac{N(\mathfrak{a})}{2}} \end{aligned}\right\} \text{ für } n \equiv 0 \pmod 2,\ \mathfrak{p}^2 \mid 2 \text{ oder } \mathfrak{p}^2 \nmid 2,\ a_i \geqq 1$$
$$\text{und für } n \equiv 1 \pmod 2,\ \mathfrak{p}^2 \mid 2,\ a_i = 1,\ a_i > 3;$$

$$\left.\begin{aligned} S_i &= (x^2-1)^{\frac{\varphi(\mathfrak{a})}{2}} \\ T_i &= [x^2(x^2-1)]^{\frac{N(\mathfrak{a})}{4}} \quad \text{für } n > 1 \\ T_i &= [x(x-2)(x^2-1)]^{\frac{N(\mathfrak{a})}{4}} \quad \text{für } n = 1 \end{aligned}\right\} \text{für } n \equiv 1 \bmod 2),\ \mathfrak{p}^2 \nmid 2,\ a_i > 1$$

gesetzt wird. Dieses Ergebnis ist die Vorallgemeinerung des RADOSschen Satzes für zusammengesetzte Idealmoduln.

3. Für $n = 1$ erhielt dieses Ergebnis H. S. VANDIVER.

4. Es sei $\mathfrak{K}$ der Körper der rationalen Zahlen. Es sei

$$a = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$$

eine rationale ganze Zahl. Nach der 2. Anwendung wird (r_j durchläuft das System aller verschiedenen, zu a teilerfremden Reste mod a)

$$\prod_{j=1}^{\varphi(a)} (x - r_j^n) \equiv \sum_{i=1}^{k} \left(\frac{a}{p_i^{\alpha_i}}\right)^{\varphi(p_i^{\alpha_i})} S_i \pmod a,$$

$$\prod_{j=1}^{a} (x - j^n) \equiv \sum_{i=1}^{k} \left(\frac{a}{p_i^{\alpha_i}}\right)^{\varphi(p_i^{\alpha_i})} T_i \pmod a,$$

wo im Falle einer ungeraden Primzahl p_i

$$S_i = (x^{\frac{p_i-1}{d_i}} - 1)^{d_i \frac{\varphi(a)}{p_i - 1}},$$

$$T_i = [x(x^{\frac{p_i-1}{d_i}} - 1)^{d_i}]^{\frac{a}{p_i}},$$

und im Falle $p_i = 2$

$$\left.\begin{aligned} S_i &= (x-1)^{\varphi(a)} \\ T_i &= (x^2-1)^{\frac{a}{2}} \end{aligned}\right\} \quad \text{für } n \equiv 0 \pmod 2, \quad a_i \geqq 1 \text{ und für } n \equiv 1 \pmod 2, \quad a_i = 1;$$

$$\left.\begin{aligned} S_i &= (x^2-1)^{\frac{\varphi(a)}{2}} \\ T_i &= [x^2(x^2-1)]^{\frac{a}{4}} \end{aligned}\right\} \quad \text{für } n \equiv 1 \pmod 2, \quad n > 1, \quad a_i > 1;$$

$$T_i = [x(x-2)(x^2-1)]^{\frac{a}{4}} \quad \text{für} \quad n = 1, \quad a_i > 1.$$

Dieses Ergebnis rührt von M. BAUER her (a. a. O. [5]).

5. Das Repräsentantensystem der $N(\mathfrak{p}^a)$ Zahlklassen mod $\mathfrak{p}^a$ unterscheidet sich vom Repräsentantensystem der zu $\mathfrak{p}^a$ teilerfremden Zahlklassen mod $\mathfrak{p}^a$ nur durch die Elemente

$$0 + \pi\tau_1^{(1)} + \pi^2\tau_1^{(2)} + \ldots + \pi^{a-1}\tau_1'^{(a-1)}, \tag{41}$$

wo die τ_1 voneinander unabhängig das Repräsentantensystem der $N(\mathfrak{p})$ Zahlklassen mod $\mathfrak{p}$ durchlaufen. Der Ausdruck (41) kann auch so geschrieben werden:

$$\tau_{a-1}\pi,$$

wo τ_{a-1} das Repräsentantensystem der $N(\mathfrak{p}^{a-1})$ Zahlklassen mod $\mathfrak{p}^{a-1}$ durchläuft. Also wird

$$\prod_{\tau_a} f(\tau_a^n) \equiv \prod_{\tau_{a-1}} f((\tau_{a-1}\pi)^n) \cdot \prod_{\varkappa_a} f(\varkappa_a^n) \pmod{\mathfrak{p}^a}.$$

Nach (19) und (20) ist aber

$$\prod_{\tau_a} f(\tau_a^n) \equiv f(0)^{N(\mathfrak{p}^{a-1})} \prod_{\varkappa_a} f(\varkappa_a^n) \pmod{\mathfrak{p}^a}.$$

Folglich wird

$$\prod_{\tau_{a-1}} f((\tau_{a-1}\pi)^n) \prod_{\varkappa_a} f(\varkappa_a^n) \equiv f(0)^{N(\mathfrak{p}^{a-1})} \prod_{\varkappa_a} f(\varkappa_a^n) \pmod{\mathfrak{p}^a}.$$

Ist $f(0) \not\equiv 0 \pmod{\mathfrak{p}}$, so sind auch $f(\varkappa_a)$ und $f(\varkappa_a^n)$ teilerfremd zu $\mathfrak{p}^a$. Wir können also durch $\prod_{\varkappa_a} f(\varkappa_a^n)$ dividieren und erhalten

$$\prod_{\tau_{a-1}} f((\tau_{a-1}\pi)^n) \equiv f(0)^{N(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}^a}.$$

Es sei hier

$$f(x) = F(X+x),$$

dann ist

$$\prod_{\tau_{a-1}} F(X+(\tau_{a-1}\pi)^n) \equiv F(X)^{N(\mathfrak{p}^{a-1})} \pmod{\mathfrak{p}^a}.$$

Für $n=1$ und einen rationalen Körper wird

$$\prod_{u=1}^{p^{a-1}} F(X+up) \equiv F(X)^{p^{a-1}} \pmod{p^a}.$$

Für $p>2$, $X=x-a$ ist dies Ergebnis (im Falle, dass $F(X)$ ganze rationale Koeffizienten besitzt) in dem Satze von S. LUBELSKI enthalten.

(*Eingegangen am 18. Dezember 1930.*)